SOFTWARE ADMINISTRATIVE RIGHTS ISSUES UPDATE

AGENDA ITEM NUMBER 22

Garry Runyans
&
Bob Bowe

The Issue

- Jan 04 IMA RCIOs surfaced update of PC applications was a burden to the DOIMs
- Most users have no power user or admin. rights
- DOIMs are having to load PC applications for the user

AR 25-1 (page 37)

r. Internet (World Wide Web (WWW)), intranets, and extranets. Official Army Web sites may exist on any of the above forms of “nets.” The use of these net communications can support execution of Army missions through information sharing and can save resources currently expended on traditional means of communication. Users are encouraged to make it their preferred and routine choice to access, develop, and exchange information. Army Web sites must be in compliance with the DOD Web site administration policy located at http://www.defenselink.mil/webmasters/ or contained within subsequent DOD directives. In addition, the following Army policies apply:

(1) Access to all forms of nets is authorized for all personnel as deemed reasonable by respective managers. Access may be implemented without further justification than this regulation.

(2) The AKO at www.us.army.mil is the primary portal for Army unclassified intranets and the NIPRNET. The AKO-S is the primary portal for classified intranets and the SIPRNET.

(a) As of July 2002, Army Web-enabled business applications will be linked to the AKO portal. Initial minimum standard to link applications to AKO is a URL link on The Army Portal. The objective standard to link applications to AKO is to use the AKO directory services for authentication as well as a URL link on The Army Portal.

(b) AKO is responsible for generating user IDs and accounts, performing authentication via secure Lightweight Directory Access Protocol (LDAP) directory services, publishing updates to the technical mechanism used for directory services, and incorporating appropriate security measures.

AR 25-2 (page 20)

e. Configuration requirements. The following policy will be the minimum used for the configuration management of all systems —

(1) Hardware and software changes to an accredited IS with an established baseline will be effected through the configuration management process.

(2) The CCB or the Configuration Management Board (CMB) for a site must approve modifying or reconfiguring the hardware of any computer system. Hardware will not be connected to any system or network without the express written consent of the IAM and the CMB or CCB. In the absence of a CCB or CMB, the appropriate commander or manager will provide the consent on the advice of the cognizant IA official.

(3) Modifying, installing, or downloading of any software on any computer system may affect system C&A and must be evaluated and approved by the IAM with the local CMB, CCB, and DAA.

(4) ISs must meet minimum levels of total system exposure. See paragraph 4-4 and DODI 8500.2 to establish baseline requirements.

AKM Goal 4

IMPLEMENTING INSTRUCTIONS FOR GOAL 4

Reduction and Webification of Applications

Purpose. To provide implementing guidance for Goal 4 of the Secretary of the Army, Chief of Staff, Army memorandum, Subject: Army Knowledge Management (AKM) Guidance Memorandum Number 2, 3 June 2002 which directs:

i. Webify. This term encompasses both Web-enabling and Web-basing applications/systems. A Web-enabled system is a system where the user can access information via a thin client browser. A Web-based system has been designed from the ground up so that all functions are performed from any Web browser, including program setup, diagnosis, data entry, report generation, and all other management activities. The following levels of webification, in ascending order, are established for reporting purposes:

1) Web Enabled. System runs on a JTA-Army -approved browser without the need to preload any other software onto the client prior to first web access (software may be downloaded as part of the login).

2) AKO-Linked. System is web enabled and linked through a page on AKO so that users can get to the system via the portal. This is the initial minimum standard that must be met NLT 31 July 2002.

3) AKO Single Sign On. System is AKO-linked and utilizes the AKO Directory Services for access authorization. A user who is logged on to the AKO portal will have access to the system without having to go through a separate system login. The interim goal will be to provide a separate system login prompt that uses the same AKO UserID/password, but this does not count as “AKO Single Sign On” status for reporting purposes.

Telephone Conference Call

- Bob Bowe
- Ted Hendy
- Sally Dixon
- David VerPlanck
- Tim Smeltzer
- Rod Frazier
- Gary Robinson
- Garry Runyans
- Tom Largent
- Andy Stanley
- Kathy Thrasher
- Steve Gibson
- Connie Teague
- Steve Naumcheff
- Bob Coker

Information

- The concern is software loaded or updated could change the libraries; thus, jeopardizing the accreditations.

Recommendations Discussed

- Provide Auto Updates similar to anti-virus software
- Automate a pull for software updates instead of a push from a web site.
- Assign elevated rights to the effected users.
- Establish an agreement with each DOIM to push PAX software updates with other updates.
- Get the DOIMs to support the requirement.
- Webify all PC applications.
- Bundle executables to minimize installs and push table updates.
- Terminal Services – Thin client
- Establish an IMA RCIO/DOIM web site for posting, testing and inclusion into SMS pushes.

And we continue to evaluate recommendations.

Questions

Comments

Concerns